another block of data. The proposed AES standard will include only a 128-bit standard length for plaintext blocks and 128, 192 and 256-bit standard lengths for the key material. --

Please delete the heading "Description of the prior art" at line 17 of page 1.

Please replace the paragraph beginning at line 20 of page 4 with the following rewritten paragraph:

--In the diagram of figure 4, reference numeral 12 designates a demultiplexer which distributes the input unencrypted data stream UD over four different paths leading to respective adder modules 14a, 14b, 14c and 14d where the first key addition is performed.--

Please replace the paragraph beginning at line 25 of page 4 with the following rewritten paragraph:

--Reference numerals 24a, 24b, 24c and 24d designates respective sets of byte registers wherein the 32-bit words subjected to the first key addition are distributed over four byte registers to be subsequently fed to respective sets of modules 34a, 34b, 34c and 34d where the S-box processing takes place.--

Please replace the paragraph beginning at line 21 of page 5 with the following rewritten paragraph:

--The main disadvantage of the prior art solutions exemplified by the arrangement shown in figure 4 lies in the complex circuitry required to implement the encryption/decryption mechanism. Such a disadvantage is particularly felt to those envisaged applications of cryptosystems adapted for use in embedded systems such as, e.g., smartcards and the like.--

Please insert the following heading at line 28 of page 5:

--Summary of the Invention--

Please replace the paragraph beginning at line 32 of page 5 with the following rewritten paragraph:

--According to the present invention, this object, as well as additional objects are achieved by means of a method and system using a transposed arrangement for the internal state array of a matrix to provide a more rapid encryption/decryption process. The present invention also provides a circuit for implementing the process.--

Please replace the paragraph beginning at line 6 of page 6 with the following rewritten paragraph:

The paragraph beginning at line 6 of page 7 has been amended as follows:

--The following description will therefore deal - by way of example only - with 128-bit blocks, as this adheres to the presently prognosticated standard.--

Please replace the paragraph beginning at line 9 of page 6 with the following rewritten paragraph:

--The invention will now be described, by a way of non limiting example, by referring to the enclosed drawings, wherein:

-Figures 1 to 4, illustrate prior art approaches for implementing the Rijndael/AES algorithm,

-Figure 5 illustrates comparison to figure 3, the basic underlying mechanism of the present invention, and

-Figure 6 is a schematic diagram of a data encryption/decryption circuit according to the present invention.--

Please replace the heading beginning at line 21 of page 6 with the following:

--Detailed Description of the Preferred Embodiments of the Present Invention--

Please replace the paragraph beginning at line 23 of page 6 with the following rewritten paragraph:

--In order to better understand the basic underlying principle of the invention, it must be recalled that Rijndael

is a secret key cryptographic algorithm working in block cipher mode. This means that it operates on blocks of data and not on single bits or bytes. The algorithm reads an entire block, processes it and then outputs the encrypted block. The decryption operates in a complementary way to re-obtain plaintext starting from encrypted data.--

Please replace the paragraph beginning at line 34 of page 8 with the following rewritten paragraph:

--Transposed Form $x_i = S_{0,i}\ S_{1,i}\ S_{2,i}\ S_{3,i}$

where x_i, $0 \leq i \leq 3$ are the words of the transposed state, and y_i, $0 \leq i \leq 3$ are the words of the transposed state after mix column transformation.--

Please replace the paragraph beginning at line 10 of page 9 with the following rewritten paragraph:

--Such a transposition requires a redefinition of most of the operations performed in a round of the algorithm, and also if the key schedule. Therefore, also the round keys must be transposed before being applied to a round providing for the use of a transposed state.--

Please replace the paragraph beginning at line 23 of page 9 with the following rewritten paragraph:

--This means that the internal behavior of the system is modified, and simplified, the only requirement to